## Claims

What is claimed is:

1. A method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterizable as a graph comprising a plurality of nodes, the method comprising the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes, such that the recipient device is thereby configurable for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.

2. The method of claim 1 wherein at least one of the nodes of the graph corresponds to a seed the possession of which permits execution of a corresponding one of the distinct portions of the cryptographic functionality.

3. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least two of the nodes.

4. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one parent node of the graph.

5. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one child node of a parent node of the graph.

6. The method of claim 1 wherein the graph comprises at least first and second root nodes.

7. The method of claim 1 wherein the graph comprises a tree having at least first and second subtrees associated with respective first and second ones of the plurality of distinct portions of the cryptographic functionality.

8. The method of claim 1 wherein the graph comprises a chain.

9. The method of claim 1 wherein the graph comprises $L$ levels of nodes, an $L$th one of the levels comprising a parent node $v_{L,1}$, and a first one of these levels comprising a set of seeds $v_{1,1}, v_{1,2}, \ldots v_{1,n}$, where $n$ is the total number of seeds, each of the seeds being derivable from the parent node.

10. The method of claim 9 wherein an $i$th node of a $k$th one of the levels is computed as $f_k(i, v_{k+1})$, where $f_k$ is a one-way function.

11. The method of claim 10 wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes.

12. The method of claim 11 wherein the $i$th node of a $j$th tuple of the $k$th level is computed as $f_k(j, i, v_{k+1,j})$.

13. The method of claim 1 wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token.

14. The method of claim 1 wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token.

15. The method of claim 14 wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds.

16. The method of claim 1 wherein the cryptographic functionality comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token.

17. The method of claim 1 wherein the cryptographic functionality comprises at least one of an ability to verify a signature and an ability to generate a signature.

18. The method of claim 1 wherein the cryptographic functionality comprises an ability to generate one or more values of a one-way chain.

19. The method of claim 1 wherein the cryptographic functionality comprises an ability to perform symmetric cryptographic operations.

20. The method of claim 1 wherein the cryptographic functionality comprises an ability to perform asymmetric cryptographic operations.

21. The method of claim 1 wherein the cryptographic functionality comprises an ability to derive one or more cryptographic keys.

22. The method of claim 1 wherein the cryptographic functionality comprises an ability to compute one or more seeds.

23. The method of claim 22 wherein at least one of the seeds corresponds to at least one of the nodes of the graph.

24. The method of claim 1 wherein the cryptographic functionality is partitioned in accordance with a subscription model which requires compliance with at least one specified criterion for transmission from the delegating device to the recipient device of the information representative of one or more of the nodes.

25. The method of claim 24 wherein compliance with the specified criterion is satisfied upon receipt of a designated payment.

26. The method of claim 1 wherein the recipient device and the delegating device collaborate to perform at least one of a cryptographic verification function and a cryptographic generation function.

27. The method of claim 26 wherein the recipient device includes only a limited computational ability associated with performance of the cryptographic function.

28. An apparatus comprising:

a processing device comprising a processor coupled to a memory;

the processing device being utilizable in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device, the cryptographic functionality being characterizable as a graph comprising a plurality of nodes;

the processing device being configurable to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit to the recipient device information representative of one or more of the nodes, such that the recipient device is thereby configurable for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.

29. An apparatus comprising:

a processing device comprising a processor coupled to a memory;

the processing device being utilizable in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device, from at least one delegating device, the cryptographic functionality being characterizable as a graph comprising a plurality of nodes;

a given set of the nodes being associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality;

the processing device being operative to receive from the delegating device information representative of one or more of the nodes, such that the processing device is thereby configurable for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.

30. A machine-readable storage medium containing one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterizable as a graph comprising a plurality of nodes, wherein the one or more software programs when executed by the delegating device implement the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes, such that the recipient device is thereby configurable for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.